A Novel Approach For Visual Cryptography Using a Watermarking Technique

Yogesh Bani¹, Dr. B. Majhi¹, Ram S. Mangrulkar¹
¹National Institute of Technology Rourkela, Orissa
yogeshbani@gmail.com

ABSTRACT
Visual Cryptography is a new cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by human, without any decryption algorithm. Here we discuss a new approach for visual cryptography with the use of a watermarking technique, which is more secure with respect to other visual cryptographic schemes. Both watermarking and visual cryptography are used to hide the secret image. However their concepts are different. For visual cryptography a set of share binary images are used to hide the content of hidden image. The hidden image can be revealed when enough share images are obtained. For watermarking the hidden image is embedded with another cover image while preserving the quality of watermarked halftone image. Proposed scheme adds the advantages of watermarking in context of visual cryptography, which makes this scheme more secure.

KEY WORDS
Secret shares, Visual cryptography, watermarking.

II. TECHNICAL WORK PREPARATION
A: Visual Cryptography: Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by humans (without computers). The first visual cryptographic technique was developed by Moni Naor and Adi Shamir in 1994 [1]. It involved breaking up the image into n shares so that only someone with all n shares could decrypt the image by overlaying each of the shares over each other. Practically, this can be done by printing each share on a separate transparency and then placing all of the transparencies on top of each other. In their technique n-1 shares reveals no information about the original image. We can achieve this by using one of following access structure schemes.

1: (2, 2) – Threshold VCS: This is a simplest threshold scheme that takes a secret image and encrypts it into two different shares that reveal the secret image when they are overlaid. No additional information is required to create this kind of access structure.

2: (2, n) – Threshold VCS: This scheme encrypts the secret image into n shares such that when any two (or more) of the shares are overlaid the secret image is revealed. The user will be prompted for n, the number of participants.

3: (n, n) – Threshold VCS: This scheme encrypts the secret image into n shares such that when all n of the shares are combined will the secret image be revealed. The user will be prompted for n, the number of participants.

4: (k, n) – Threshold VCS: This scheme encrypts the secret image into n shares such that when any group of at least k shares are overlaid the secret image will be revealed. The user will be prompted for k, the threshold, and n, the number of participants.

Figure 1 shows two of the several approaches for (2, 2) – Threshold VCS. In this particular figure first approach shows that each pixel is broken into two sub pixels. Let B shows black pixel and T shows Transparent (White) pixel. Each share will be taken into different transparencies. When we place both transparencies on top of each other we get following combinations, for black pixel BT+TB=BB or BT+BT=BB and for white pixel BT+BT=BT or TB+TB=TB. Similarly second approach is given where each pixel is broken into four sub pixels. We can achieve ⁴C₂=6 different cases for this approach.

B: Watermarking in perspective of visual cryptography
The process of embedding information into another object/signal can be termed as watermarking. We can utilize watermarking for generating the shares [3]. Rest process will be...
same as in basic approach of visual cryptography. For this we can use following algorithm.

1. Each pixel is broken into two sub pixels as follows.

<table>
<thead>
<tr>
<th>First Share</th>
<th>Second Share</th>
<th>Resultant Block</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
</tr>
<tr>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
</tr>
</tbody>
</table>

For black

<table>
<thead>
<tr>
<th>First Share</th>
<th>Second Share</th>
<th>Resultant Block</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
</tr>
<tr>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
</tr>
</tbody>
</table>

For white

2. Each pixel is broken into four sub pixels as follows.

<table>
<thead>
<tr>
<th>First Share</th>
<th>Second Share</th>
<th>Resultant Block</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
</tr>
<tr>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>First Share</th>
<th>Second Share</th>
<th>Resultant Block</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
</tr>
<tr>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
</tr>
</tbody>
</table>

A: Visual Cryptography Encryption
In this very first phase we will do visual cryptography encryption. It consists generation of shares using any basic visual cryptography model. Visual cryptographic solutions operate on binary inputs. Therefore, natural (continuous-tone) images must be first converted into halftone images by using the density of the net dots to simulate the original gray or color levels in the target binary representation. For Halftoning we can use any halftoning technique as error diffusion, thresholding, ordered dithering [4,6] etc. So the result of this phase will be different unintelligible shares of black and white pixels.

B: Watermarking
This is the second phase of our approach which will embed our shares generated from the first phase into some cover images. For watermarking we will use Data Hiding by Conjugate Error Diffusion (DHCED) algorithm discussed under II.B. Using watermarking will give an added advantage of double security on other visual cryptographic approaches. Result of this phase will be different meaningful shares consisting some cover images.

C: Visual Cryptographic Decryption
This is the last phase of proposed scheme. In this phase we will do visual cryptographic decryption. As we know that visual cryptographic decryption does not need any type of decryption algorithm or computation. It uses human visual system for decryption which is the core advantage for which visual cryptography was developed. We will have different shares embedded in some cover image as the result of second phase. Now we can decrypt the original secret image by overlapping of shares. The result of this phase will be an image consisting secret image as well as cover image. Figure 2 is the structure of proposed scheme.

Figure 1: Visual Cryptography

Data Hiding by Conjugate Error Diffusion (DHCED) Algorithm [2]: Let H is the image to be hidden (Secret image). X is the cover image for H. X1 is the error diffused (Halftone) image of X, which will work as first share. Let Hb is the collection of location of all black pixels in H and Hw is the collection of location of all white pixels in H. We will use h(i, j) and x1(i, j) to represent the pixels at location (i, j) of H and X1 respectively.

\[ v(i, j) = \begin{cases} \text{black} & \text{if } (i, j) \in H_b, \text{the pixel } x_2(i, j) \text{ in } X_2 \text{ is favored to be identical to the collocated pixel } x_1(i, j) \text{ in } X_1. \\
\text{white} & \text{if } (i, j) \in H_w, \text{the pixel } x_2(i, j) \text{ in } X_2 \text{ is favored to be conjugate of the collocated pixel } x_1(i, j) \text{ in } X_1. 
\end{cases} \]

After overlapping of shares X1 and X2 we can reveal secret image H as well as cover image X.

III. PROPOSED SCHEME
We are proposing a new scheme for visual cryptography which will use watermarking technique to embed the generated shares into any cover image. Proposed scheme consists three different phase.

IV. SIMULATION RESULTS
Figure 3 and figure 4 are the simulation results what we have achieved till now. Here we have used MATLAB for the implementation. Figure 3 shows the results of basic visual cryptographic model using (2, 2) threshold VCS access.
structure scheme. Figure 4 shows the results of proposed visual cryptography using a watermarking technique.

V. CONCLUSION
Visual cryptography is the current area of research where lots of scope exists. Currently this particular cryptographic technique is being used by several big countries like USA, Russia, and China etc for secretly transfer of hand written documents, financial documents, text images, internet voting etc. There are many possible enhancements and extensions exist of the basic visual cryptographic model introduced till now. One such enhancement we are trying to do. There are other areas also in visual cryptography which are still open where no satisfactory results yet achieved as color visual cryptography, enhancement of image shares with respect to contrast, size, quality and clarity of revealed image. Researchers are still busy for finding the new application where visual cryptography can be used.

VI. ACKNOWLEDGMENT
The authors gratefully acknowledge the contributions of M. Naor, A. Shamir, Ming Sun Fu and Oscar C. Au for their work in the field of visual cryptography.

VII. REFERENCES

VIII. BIOGRAPHIES
Yogesh Bani was born in Almora city in Uttarakhand (India) on January 01, 1984. He did his B.Tech. in Computer Science & Engg. from Graphic Era Institute of Technology Dehradun. Currently he is pursuing M.Tech. in Computer Science & Engg. from National Institute of Technology Rourkela. He has published one paper in National Conference. His areas of interest are visual cryptography and software engineering.

Dr. B. Majhi was born on April 14, 1963. He received his M.Tech. and Ph.D in Computer Science and Engg from National Institute of Technology Rourkela. He has professional membership of FIETE, LMCSI, AMIE (India). Currently he is a Professor and Head of the Computer Science & Engg. Department in National Institute of Technology Rourkela. He has 19 years of teaching experience. He has published 31 papers in national and international conferences and 13 papers in journals. His area of interest includes Soft computing, image processing, programming languages and system programming.

Figure 3: Simulation of basic visual cryptography (a) Secret image to be hidden (b) First share (c) Second share (d) Revealed image after overlapping of share (a) and share (b).
Figure 4: Simulation of Visual Cryptography and watermarking (a) Secret image to be hidden (b) Cover image (c) First share (d) Second share